

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

**CIVIL MINUTES - GENERAL**

Case No. SACV 22-1164 JVS (ADSx) Date April 19, 2023

Title In re: Illuminate Education Data Security Incident Litigation

Present: The **James V. Selna, U.S. District Court Judge**  
Honorable

Elsa Vargas

Not Present

Deputy Clerk

Court Reporter

Attorneys Present for Plaintiffs:

Attorneys Present for Defendants:

Not Present

Not Present

**Proceedings: [IN CHAMBERS] Order Regarding Motion to Dismiss [61]**

Defendant, Illuminate Education, Inc. d/b/a Pupil Path (“Illuminate”), moves to dismiss the consolidated complaint. (Mot., Dkt. No. 61.) Plaintiffs<sup>1</sup> opposed. (Opp’n, Dkt. No. 75.) Illuminate replied. (Reply, Dkt. No. 77.) The Court vacated the hearing. Fed R. Civ. P. 78; L.R. 7-15.

For the following reasons, the Court **GRANTS in part and DENIES in part as moot** the motion. The Court **GRANTS** Plaintiffs twenty-one (21) days’ leave to amend.

**I. BACKGROUND**

Illuminate is a software company that services 17 million students in 5,200 schools and districts across all 50 states. (Compl. ¶¶ 1–2.) Illuminate offers several products that requires the collection of students’ personal information, including names, birth dates, class schedules, behavioral records, and health and socioeconomic information. (*Id.* ¶¶ 3–5.) On January 8, 2022, Illuminate became aware that an unauthorized third party gained access to Illuminate’s databases containing personally identifiable information (“PII”) and protected health information (“PHI”) of students. (*Id.* ¶ 6.) Illuminate conducted an investigation and confirmed unauthorized access took place between December 28, 2021, and January 8, 2022 (the “Data Breach”). (*Id.* ¶ 27.) The Data Breach was a result of an unauthorized access to one of Illuminate’s platforms used in K-

---

<sup>1</sup> Plaintiffs are Lucas Cranor (“Cranor”), Kristen Weiland (“Weiland”), Anastasiya Kisil (“Kisil”), Tara Chambers (“Chambers”), Janene Vitro (“Vitro”), Sarah Chung (“Chung”), and Lorraine Deniz (“Deniz”) (collectively, “Plaintiffs”). Plaintiffs bring this action individually and behalf of all others similarly situated. (*See* Consolidated Complaint (“Compl.”), Dkt. No 57.) Although Chung’s case was consolidated on this docket, she is absent from the parties’ present briefing. (Dkt. No. 54.)

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. SACV 22-1164 JVS (ADSx) Date April 19, 2023

Title In re: Illuminate Education Data Security Incident Litigation

12 school districts. (*Id.* ¶ 28.) Information leaked included student academic, behavior, and demographic information. (*Id.* ¶ 32 (listing the information leaked).) The Data Breach affected over three million students, primarily students enrolled during 2021–2022, and possibly as early as 2016. (*Id.* ¶¶ 30–31.) Illuminate did not notify schools until late March 2022. (*Id.* ¶ 8.) Plaintiffs bring this action individually and on behalf of other class members. (*Id.* ¶ 15.)

**II. LEGAL STANDARD**

*A. Motion to Dismiss Pursuant to Rule 12(b)(1)*

Dismissal is proper when a plaintiff fails to properly plead subject matter jurisdiction in the complaint. Fed. R. Civ. P. 12(b)(1). A “jurisdictional attack may be facial or factual.” *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). If the challenge is based solely upon the allegations in the complaint (a “facial attack”), the court generally presumes the allegations in the complaint are true. *Id.*; *Warren v. Fox Family Worldwide, Inc.*, 328 F.3d 1136, 1139 (9th Cir. 2003). If instead the challenge disputes the truth of the allegations that would otherwise invoke federal jurisdiction, the challenger has raised a “factual attack,” and the court may review evidence beyond the confines of the complaint without assuming the truth of the plaintiff’s allegations. *Safe Air*, 373 F.3d at 1039. The plaintiff bears the burden of establishing subject matter jurisdiction. *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994).

Pursuant to Article III of the Constitution, the Court’s jurisdiction over the case “depends on the existence of a ‘case or controversy.’” *GTE Cal., Inc. v. FCC*, 39 F.3d 940, 945 (9th Cir. 1994). A “case or controversy” exists only if a plaintiff has standing to bring the claim. *Nelson v. NASA*, 530 F.3d 865, 873 (9th Cir. 2008), *rev’d on other grounds*, 562 U.S. 134 (2011). To have standing, “a plaintiff must show (1) it has suffered an ‘injury in fact’ that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that their injury will be redressed by a favorable decision.” *Friends of the Earth, Inc. v. Laidlaw Env’tl. Servs., Inc.*, 528 U.S. 167, 180–81 (2000); *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992); *Nelson*, 530 F.3d at 873. “[P]laintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages).” *TransUnion LLC v. Ramirez*, 141 S.

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. SACV 22-1164 JVS (ADSx) Date April 19, 2023

Title In re: Illuminate Education Data Security Incident Litigation

Ct. 2190, 2208 (2021).

*B. Motion to Dismiss Pursuant to Rule 12(b)(6)*

Under Rule 12(b)(6), a defendant may move to dismiss for failure to state a claim upon which relief can be granted. A plaintiff must state “enough facts to state a claim to relief that is plausible on its face.” Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). A claim has “facial plausibility” if the plaintiff pleads facts that “allow” the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009).

In resolving a 12(b)(6) motion under Twombly, the Court must follow a two-pronged approach. First, the Court must accept all well-pleaded factual allegations as true, but “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” Iqbal, 556 U.S. at 678. Nor must the Court “accept as true a legal conclusion couched as a factual allegation.” Id. at 678–80 (quoting Twombly, 550 U.S. at 555). Second, assuming the veracity of well-pleaded factual allegations, the Court must “determine whether they plausibly give rise to an entitlement to relief.” Id. at 679. This determination is context-specific, requiring the Court to draw on its experience and common sense, but there is no plausibility “where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct.” Id.

### III. DISCUSSION

*A. Motion to Dismiss Pursuant to Rule 12(b)(1)*

An injury, for the purposes of standing, is concrete when it is “real, and not abstract.” TransUnion LLC, 141 S. Ct. at 2204. Illuminate argues Plaintiffs’ “four buckets” of harm do not establish a concrete injury. (Mot. at 5–13.)

#### 1. Whether Plaintiffs have plausibly alleged actual identity theft

Illuminate argues Plaintiffs have not plausibly alleged any actual identity theft. (Mot. at 7–8.) At most, two Plaintiffs allege their accounts were hacked in some form. Chambers alleges her Amazon and PayPal accounts were hacked. (Compl. ¶ 103.) Vitro

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. SACV 22-1164 JVS (ADSx) Date April 19, 2023

Title In re: Illuminate Education Data Security Incident Litigation

alleges “her online information [was] hacked where the hacker was able to charge her debit card on a fake website.” (Id. ¶ 115.)

Plaintiffs allege they are “concerned” that their or their child’s social security numbers were breached but do not actually allege social security numbers were part of the Data Breach. (See, e.g., Compl. ¶¶ 73, 83, 95, 107, 119, 132.) Plaintiffs allege students’ academic, behavior, and demographic information was leaked as part of the Data Breach. (Id. ¶ 32.) But notably, Plaintiffs do not allege social security, credit card, or bank information was leaked. (Id.) And as Illuminate points out, the letters Illuminate sent to Plaintiffs expressly indicate “Social Security numbers and financial information were not at risk as a result of this event.” (See Mot. Ex. 1, Dkt. No. 61-3 (notice letter to Chambers dated July 29, 2022); Ex. 2, Dkt. No. 61-4 (notice letter to Vitro dated July 29, 2022); Ex. 3, Dkt. No. 65-5 (notice letter to Cranor dated April 29, 2022).)<sup>2</sup> Taken together, the facts as alleged, do not show Plaintiffs’ financial information or social security numbers were ever compromised. As such, it’s unclear how Vitro’s allegation that someone charged her debit card on a fake website can be a result of the data breach. See Greenstein v. Noblr Reciprocal Exch., 585 F. Supp. 3d 1220, 1227–28 (N.D. Cal. 2022) (“The Court questions whether attackers would be able to use that limited information to set up credit or debit accounts without the addition of more, highly sensitive personal information such as social security numbers.”). On the other hand, it’s possible the leaked information potentially allowed an individual to recover passwords to Chambers’ Amazon and PayPal accounts. In any event, the Court is left to speculate, based on the allegations and facts, as to whether any actual identity theft occurred based on information leaked in the Data Breach.

Plaintiffs cite only one case in support of their position on this issue, Walters v. Kimpton Hotel & Restaurant Group, LLC, 2017 WL 1398660 (N.D. Cal. Apr. 13, 2017). (Opp’n at 7.) There, the district court disagreed that the “plaintiff must actually suffer the

---

<sup>2</sup> The referenced exhibits are not attached to the Complaint. But both parties rely on the letters in their briefing. Courts may consider documents “whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the [plaintiff’s] pleading” . . . [or documents] in which the plaintiff’s claim depends on the contents of a document, the defendant attaches the document to its motion to dismiss, and the parties do not dispute the authenticity of the document, even though the plaintiff does not explicitly allege the contents of that document in the complaint.” Knievel v. ESPN, 393 F.3d 1068, 1076 (9th Cir. 2005).

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. SACV 22-1164 JVS (ADSx) Date April 19, 2023

Title In re: Illuminate Education Data Security Incident Litigation

misuse of his data or an unauthorized charge before he has an injury for standing purposes.” Walters, 2017 WL 1398660, at \*1. But the Supreme Court’s holding in TransUnion LLC casts doubt on that reasoning. 141 S. Ct. at 2211–12 (noting the injury must “materialize”). And as discussed above, the factual allegations do not actually create a nexus between the information leaked and the alleged harm (*i.e.*, Chambers’ and Vitro’s allegations).

Relatedly, Cranor, Weiland, Chambers, Vitro, and Deniz allege they have “noticed a substantial uptick in unwanted spam telephone calls and text messages since the Data Breach.” (Compl. ¶¶ 72, 82, 103, 115, 131.) Illuminate argues this is insufficient to establish standing. The Court agrees. Receipt of spam, absent any other injury, is insufficient to establish an injury for the purposes of standing. *See Jackson v. Loews Hotels, Inc.*, 2019 WL 6721637, at \*4 (C.D. Cal. July 24, 2019).

Accordingly, Plaintiffs have not established standing based on actual identity theft.

**2. Whether Plaintiffs have plausibly alleged a material risk of future identity theft**

“[P]laintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages).” TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2208 (2021). “[T]he risk of future harm on its own does not support Article III standing. . . .” *Id.* at 2214. As the Ninth Circuit later reiterated, “the Supreme Court is clear that where a risk of future harm has not yet materialized, the ‘plaintiffs’ argument for standing for their damages claims based on an asserted risk of future harm is unavailing.” Bock v. Washington, 33 F.4th 1139, 1145 (9th Cir. 2022) (quoting TransUnion LLC, 141 S. Ct. at 2211). Such a harm can support standing if the harm materializes or causes some other injury. TransUnion LLC, 141 S. Ct. at 2211.

Plaintiffs seek money damages. (Compl. ¶ B.) Plaintiffs allege, as a result of the Data Breach, they “have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, . . .” (Compl. ¶ 151.) But Plaintiffs do not allege anything more. As discussed above, Plaintiffs fail to establish any actual identity theft related to the Data Breach and thus the harm has not materialized. Likewise, Plaintiffs fail to allege how the information leaked in the Data Breach (*i.e.*,

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. SACV 22-1164 JVS (ADSx) Date April 19, 2023

Title In re: Illuminate Education Data Security Incident Litigation

academic and behavioral information) puts them at harm or risk, particularly credible and immediate risk of harm. Plaintiffs' allegations are conclusory at best. For example, Plaintiffs cite to cases and articles indicating children are at a higher risk of identity theft. (Compl. ¶¶ 39–43.) But Plaintiffs fail to make any connection at all between the information leaked in the Data Breach and the alleged harms and dangers. Plaintiffs' allegations do not “demonstrate that the risk of future harm materialized.” TransUnion LLC, 141 S. Ct. at 2211; see, e.g., I.C. v. Zynga, Inc., 600 F. Supp. 3d 1034, 1051 (N.D. Cal. 2022).

Plaintiffs' reliance on Krottner v. Starbucks Corporation, 628 F.3d 1139 (9th Cir. 2010) and Zappos.com, Inc. v. Customer Data Security Breach Litigation (“Zappos”), 888 F.3d 1020 (9th Cir. 2018), is unpersuasive given the Supreme Court's holding in TransUnion LLC. Notwithstanding TransUnion, LLC, both Krottner and Zappos are distinguishable on the facts. In Krottner, employee names, addresses, and social security numbers were stored on laptops and the laptops were stolen. 628 F.3d at 1140. Accordingly, the Ninth Circuit held this sufficiently established standing because there was a “credible threat of harm” that is “both real and immediate, not conjectural or hypothetical.” Id. at 1143; see also Zappos, 888 F.3d at 1026 (“The Krottner laptop thief had all the information he needed to open accounts or spend money in the plaintiffs' names—actions that Krottner collectively treats as ‘identity theft.’”). Conversely, Plaintiffs here do not allege a real and immediate credible threat of harm related to the information leaked in the Data Breach. See Zappos, 888 F.3d at 1027 (“The threat would have been ‘far less credible,’ we explained, ‘if no laptop had been stolen, and [they] had sued based on the risk that it would be stolen at some point in the future.’”). Just as importantly, social security numbers are not at issue here. In Zappos, stolen information *including* credit card information “gave hackers the means to commit fraud or identity theft.” Id. at 1027. Plaintiffs make no allegation to show the information at hand creates a real and immediate credible threat of harm. To be clear, Plaintiffs do not lack standing simply because the Data Breach did not involve credit card numbers, social security numbers, or other financial information. Nor does the Court's order suggest academic and behavioral information is not important or private. Rather, Plaintiffs merely conclusory allege risk of future harm without more. They make no connection between the personal information leaked and the harms alleged, nor do Plaintiffs allege such harms are real, immediate, and concrete.

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. SACV 22-1164 JVS (ADSx) Date April 19, 2023

Title In re: Illuminate Education Data Security Incident Litigation

Plaintiffs' reliance on Clemens v. ExecuPharm Inc., 48 F.4th 146 (3rd Cir. 2022) and In re Blackbaud, Inc., Customer Data Breach Litigation, 2021 WL 2718439 (D.S.C. July 1, 2021), is unhelpful for similar reasons. Both cases involved different types of personal information, namely social security numbers, bank account information, credit card information, and insurance and tax information. And in Clemens, imminence was established given the sophisticated phishing attacks occurring. 48 F.4th at 157. Additionally, the Court finds Plaintiffs' reliance on Stallone v. Farmers Group, 2022 WL 10091489 (D. Nev. Oct. 15, 2022), is unpersuasive given the courts limited discussion of TransUnion LLC.

Plaintiffs also seek injunctive relief. (Compl. ¶ C.) "[A] person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." TransUnion LLC, 141 S. Ct. at 2211 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013)). But for the same reasons discussed above, Plaintiffs' allegations fail to establish a risk of harm that is imminent and substantial. Plaintiffs allege theirs or their child's personal information (e.g., academic and behavioral information) was leaked in the Data Breach. (Compl. ¶ 32.) Then Plaintiffs cite articles and studies showing how "[c]hildren's data is particularly attractive to data thieves and can have long-lasting effects on the child's financial history and identity." (Id. ¶ 39.) And finally, Plaintiffs conclusory allege a "substantially increased risk of fraud, identity theft, and misuse" resulting from the Data Breach. (See, e.g., Compl. ¶ 118.) But Plaintiffs do not explain how the information leaked in the Data Breach creates a risk that is imminent and substantial. See, e.g., Zynga, Inc., 600 F. Supp. 3d at 1055.

Accordingly, Plaintiffs have no standing where the harm is based on risk of future identity theft and fraud.

### 3. Whether Plaintiffs have plausibly alleged harms derivative of the allegations of future harm

A plaintiff does not have standing where "they cannot demonstrate that the future injury they purportedly fear is certainly impending . . . ." Clapper, 568 U.S. at 422. Plaintiffs allege "loss of time" implementing mitigation measures related to the Data Breach and emotional harms. (See Compl. ¶¶ 148, 159.) But as discussed above, Plaintiffs fail to allege any certainly impending harms. Accordingly, time lost mitigating

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. SACV 22-1164 JVS (ADSx) Date April 19, 2023

Title In re: Illuminate Education Data Security Incident Litigation

the Data Breach is insufficient to establish standing here. See Antman v. Uber Tech., Inc., 2015 WL 6123054, at \*11 (N.D. Cal. Oct. 19, 2015) (“[M]itigation expenses do not qualify as injury; the risk of identity theft must first be real and imminent, and not speculative, before mitigation costs establish injury in fact.”) (collecting cases); see also Payne v. Off. of the Comm’r of Baseball, 705 Fed. App’x 654, 655 (9th Cir. 2017) (rejecting the argument that “general anxiety” as to future harms is sufficient to establish injury-in-fact). To the extent Plaintiffs allegations relate to mitigation measures for possible future harms or identity theft, such allegations fail to establish standing. See Clapper, 568 U.S. at 402 (“[Plaintiffs] cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending.”).

Accordingly, Plaintiffs have no standing where the harm is based on time lost on mitigation measures or emotional distress.

**4. Whether Plaintiffs have plausibly alleged a loss of value of information or privacy**

“The Ninth Circuit has recognized diminution in value of personal information as a viable theory of damages under state contract law.” Svenson v. Google Inc., 2016 WL 8943301, at \*9 (N.D. Cal. Dec. 21, 2016) (citing In re Facebook Privacy Litig., 572 Fed. App’x 494, 494 (9th Cir. 2014)). This requires showing “both the existence of a market for her personal information and an impairment of her ability to participate in that market.” Id.

Plaintiffs argue they need only prove the existence of a market for personal information *or* an impairment of an ability to participate in the market for their personal information. (Opp’n at 8–9. (citing Stallone v. Farmers Group, Inc., 2022 WL 10091489, at \*6 (D. Nev. Oct. 15, 2022) (“These pleading requirements, that a plaintiff must establish both the existence of a market for their PII and an impairment of their ability to participate in that market is not supported by Ninth Circuit precedent, and other district courts in this Circuit have rejected them.”)).) The Court need not address this purported split as Plaintiffs fail in any event to sufficiently allege either requirement.

Plaintiffs allege they have “suffered actual injury in the form of damages to and diminution of the value of [their] Private information.” (See Compl. ¶¶ 69, 79, 91, 102, 114, 127; see also Opp’n at 8–9.) Plaintiffs also allege private information can be traded

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

**CIVIL MINUTES - GENERAL**

Case No. SACV 22-1164 JVS (ADSx) Date April 19, 2023

Title In re: Illuminate Education Data Security Incident Litigation

on the dark web and “cyber black-market” generally. (Compl. ¶ 143.) But these allegations are entirely conclusory. Plaintiffs do not explain how or why their information has lost value. See, e.g., Patterson v. Med. Rev. Inst. of Am., 2022 WL 2267673, at \*3 (N.D. Cal. June 23, 2022). And Plaintiffs do not allege a market for Personal Information (*i.e.*, school and academic information) nor their inability to participate in such a market. Any of Plaintiffs allegations related to such are conclusory regardless of whether the above referenced pleading requirement is conjunctive or disjunctive.

As to loss privacy, “[s]everal other federal courts have similarly rejected the argument that a loss of privacy arising from the theft of non-sensitive personal information, standing alone, supports Article III standing.” Kim v. McDonald’s USA, LLC, 2022 WL 4482826, at \*5 (N.D. Ill. Sept. 27, 2022) (collecting cases). Illuminate argues and Plaintiffs do not dispute the allegations of loss of privacy do not sufficiently establish standing. (Mot. at 12–13.)

Accordingly, Plaintiffs have no standing related to loss of value of information or privacy.

## 5. Conclusion

Based on the foregoing, Plaintiffs failed to establish standing. Accordingly, the Court **GRANTS** the motion to dismiss pursuant to Rule 12(b)(1). Because the Court grants the motion to dismiss as to standing, the Court need not analyze Illuminate’s motion to dismiss based on failure to state a claim or choice-of-law analysis. Thus, the Court **DENIES** the motion to dismiss pursuant to Rule 12(b)(6) as moot.

### *B. Leave to Amend*

The Court finds Plaintiffs may be able to cure the deficiencies identified. As such, the Court grants Plaintiffs leave to amend. See Warth v. Seldin, 422 U.S. 490, 501–02 (1975) (noting courts should ordinarily grant leave to amend when granting for the first time a motion to dismiss for lack of standing).

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

**CIVIL MINUTES - GENERAL**

Case No. SACV 22-1164 JVS (ADSx) Date April 19, 2023

Title In re: Illuminate Education Data Security Incident Litigation

While the Court makes no ruling on the adequacy of Plaintiffs' claims under Rule 12(b)(6), Plaintiffs are advised to consider the alleged deficiencies identified by Illuminate when amending their complaint.

Accordingly, the Court **GRANTS** Plaintiffs twenty-one (21) days' leave to amend.

**IV. CONCLUSION**

For the foregoing reasons, the Court **GRANTS in part and DENIES in part as moot** the motion. The Court **GRANTS** Plaintiffs twenty-one (21) days' leave to amend.